



Network Computing Darkreading

Welcome Guest

[Login to your account](#)

[Advertise](#)

[About Us](#)

SECTIONS ▼



[Authors](#)

[Slideshows](#)

[Video](#)

[Reports](#)

[White Papers](#)

[Events](#)

[Black Hat](#)

[Attacks/Breaches](#)

[App Sec](#)

[Cloud](#)

[Endpoint](#)

[Mobile](#)

[Perimeter](#)

[Risk](#)

[Operations](#)

[Analytics](#)

[Vulns/Threats](#)

[Threat Intelligence](#)

[Careers and People](#)

[IOT](#)



[Login to your account](#)

[Register](#)

[About Us](#)

[Advertise](#)



Search Dark Reading



[Facebook](#)

[Twitter](#)

[LinkedIn](#)

[Google+](#)

[RSS](#)



[Register](#)



LEARN
MORE ▶

DARKReading

Join us live at

InteropITX

Search Dark Reading



[Analytics](#)
[Attacks / Breaches](#)
[App Sec](#)
[Careers & People](#)
[Cloud](#)
[Endpoint](#)
[IoT](#)
[Mobile](#)
[Operations](#)
[Perimeter](#)
[Risk](#)
[Threat Intelligence](#)
[Vulns / Threats](#)

Attacks/Breaches

3/1/2018
06:30 PM



Jai Vijayan
News

Connect Directly



0 comments

[Comment
Now](#)

[Login](#)



Like

Tweet

Share

G+

Number of Sites Hosting Cryptocurrency Miners Surges 725% in 4 Months

The dramatic increase in cryptocurrency prices, especially for Monero, is behind the sudden explosive growth, says Cyren.

A new report from security vendor Cyren this week confirms assumptions about the recent explosive growth in the number of websites that host cryptocurrency mining software.

Cyren monitored a sample of 500,000 websites between September 2017 and January 2018 and found a 725% increase in the number of domains running cryptocurrency scripts on one or more pages over that period.

As fast as that growth has been, it's still accelerating. According to Cyren, the number of sites knowingly or unknowingly hosting software for mining cryptocurrency registered a threefold jump between last September and October. It plateaued in November before nearly doubling in December and then doubling again in January.

In other words, half the total increase has happened in just the last two months, suggesting that the growth is accelerating, the [company said](#). A total of 7,281 — about 1.4% of the 500,000 websites that Cyren monitored — ran cryptocoin mining scripts as of January 2018.

Much of the growth is being fueled by the insane run-up in cryptocurrency prices in recent months. For instance, the value of Monero, the most widely mined cryptocurrency at the moment, increased by 250% during the four-month period when Cyren was monitoring the websites.

Tinna Thuridur Sigurdardottir, malware analyst at Cyren, says the sites hosting cryptocoin mining tools include both high-traffic and low-traffic destinations. "Most of the sites we've seen are not in the top 10,000 sites globally," says Sigurdardottir. "But there are instances of top 10,000 sites."

Sites can host cryptocurrency mining tools knowingly or — as in a growing number of cases — unknowingly.

A growing number of website operators have begun voluntarily installing cryptocurrency mining software on their sites as a way to supplement revenues generated by ads. As Sigurdardottir notes, two well-known websites doing this are Showtime and Salon magazine.

The operators make money by allowing the mining software to use the systems belonging to website visitors to mine for cryptocurrency. Some sites alert users to the mining activity, while many others do it surreptitiously.

In many other cases, cybercriminals have begun installing mining tools in websites without the knowledge of the operators. They are then quietly using the computing resources of people visiting these sites to mine for digital currency.

Mining tools often consume a lot of CPU resources and can seriously affect system performance. Not all cryptocurrency miners are scripts, Cyren said in its report. Some are executables that could be used at any time to download and install something other than a cryptocurrency mining script.

Cryptocurrency miners are extremely easy for site owners to install and super easy for attackers as well once they've hacked a website through usual techniques, Sigurdardottir says. The proliferation of simple JavaScript code from sources such as Coinhive and other Monero miners like Crypto-Loot and deepMiner makes embedding script on a website relatively simple, she says.

Often, all website owners — or attackers — need to do embed a miner in a site is insert two lines of JavaScript. "Coinhive even offers generic code for a website owner to copy and paste into the website's HTML code, replacing 'SITE_KEY' with their own Coinhive site key," Sigurdardottir notes. "Once the code is embedded, all that is required is a visitor coming to the site and spending time there."



Sponsored Content The Ransomware Survival Handbook

A guide to prevention, response, and recovery

Brought to you by Barkly

Sigurdardottir says it is impossible to know whether sites that are hosting cryptocurrency mining tools are doing so unknowingly or unknowingly without speaking to each operator individually. But attackers have broken into everything from thousands of government sites to basic WordPress sites to embed mining software in recent months, she says.

One entity that has been making these miners widely available is Coinhive.com, whose Coinhive Monero miner is easily the most widely deployed in-browser miner in use. Though Coinhive by itself is a legitimate mining tool, many anti-malware products have begun blocking it because the tool is often embedded in sites without the site owner's knowledge.

Other less widely distributed miners include Crypto-Loot and Coinhave, both of which are also Monero miners, says Sigurdardottir. "Monero is the most common currency," she says. "Monero bills itself as a 'secure, private, and untraceable cryptocurrency,' employing a technology that makes it virtually impossible to track transactions to any individual or IP address."

Related content:

- [Crypto-Mining Attacks Emerge as the New Big Threat to Enterprises](#)
- [7 Cryptominers & Cryptomining Botnets You Can't Ignore](#)
- [Cybercriminals Employ 'Driveby' Cryptocurrency Mining](#)
- [FBI Director: Cryptocurrency, Nation-State Attacks, Among Agency's Top Cybersecurity Concerns](#)



Black Hat Asia returns to Singapore with hands-on technical Trainings, cutting-edge Briefings, Arsenal open-source tool demonstrations, top-tier

solutions and service providers in the Business Hall. Click for information on the [conference](#) and [to register](#).

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year ... [View Full Bio](#)

[Comment](#) | [Email This](#) | [Print](#) | [RSS](#)

More Insights

Webcasts

Shrink the Attack Surface & Make Faster, More Accurate Calls

[Dark Reading] Cybersecurity Crash Course

More Webcasts

White Papers

8 Nation-State Hacking Groups to Watch in 2018

Whaling: Anatomy of an Email Attack

More White Papers

Reports

[Forrester's Report] The State of Application Security: 2018 & Beyond

[Strategic Security Report] Navigating the Threat Intelligence Maze

More Reports

Comments

Newest First | [Oldest First](#) | [Threaded View](#)

[Be the first to post a comment regarding this story.](#)

Related Content

Sponsored by

RESOURCES

VIDEO

TWITTER

Global CISO Report

The role of the CISO is growing in importance, as is the need to have an enterprise-wide IT security strategy that supports the company's missions and ...

The Hunt for IoT - The Rise of Thingbots

F5 Labs has been tracking the hunt for IoT devices, the associated botnets being built from this activity, and the attacks they launch for the past year and a half.

How Quantum Computing Will Change Browser Encryption

The crypto community has been trying to prepare for the transition to "quantum-resistant" algorithms-- that is, algorithms ...

Phishing - The Secret of its Success and What You Can Do to Stop It

Phishing has proved so successful that it is now the number one attack vector. The Anti-Phishing Working Group reports that...

Lessons Learned From a Decade of Data Breaches

F5 Labs researched 433 breach cases spanning 12 years, 37 industries, and 27 countries to discover patterns in...



Hot Topics

Editors' Choice

4

[Pragmatic Security: 20 Signs You Are 'Boiling the Ocean'](#)

Joshua Goldfarb, Co-founder & Chief Product
Officer, IDDRA, 3/6/2018

[⁴
How Guccifer 2.0 Got 'Punk'd' by a Security
Researcher](#)

Kelly Jackson Higgins, Executive Editor at Dark
Reading, 3/8/2018

[³
Connected Cars Pose New Security Challenges](#)

James Plouffe, Lead Architect at MobileIron,
3/6/2018



[Subscribe to Newsletters](#)

Live Events

Webinars



UBM
Tech

More UBM Tech
Live Events

**Interop ITX: The Independent Conference For Tech
Leaders (April 30 - May 4 In Las Vegas)**

**Enterprise Connect Conference and Expo: March
12-15**

**Speech Technologies - New Track at Enterprise
Connect!**

White Papers

[8 Nation-State Hacking Groups to Watch in 2018](#)

[Whaling: Anatomy of an Email Attack](#)

[GDPR - Friend or Foe?](#)

[The Equifax Breach & How Software Composition Analysis Cloud Have Prevented It](#)

[The Main AppSec Tech to Adopt in 2018](#)

More White Papers



Video



All Videos

Cartoon Contest

Write a Caption, Win a Starbucks Card! [Click Here](#)

How Security Metrics Fail - Attacking De



Latest Comment: [This comment is waiting for review by our moderators.](#)

Cartoon Archive

Current Issue



How to Cope with the IT Security Skills Shortage

Most enterprises don't have all the in-house skills they need to meet the rising threat from online attackers. Here are some tips on ways to beat the shortage.

Download This Issue!

[Back Issues](#) | [Must Reads](#)

[Flash Poll](#)

Has the U.S. political climate caused you to make infosecurity-related changes to your disaster recovery/business continuity plans?

- ☐ Yes
- ☐ No
- ☐ No but we are considering it
- ☐ Still waiting for cybersecurity guidance from Trump admin EO
- ☐ Don't know
- ☐ Other (Please explain in the comments)

Submit

[All Polls](#)

[Reports](#)



[Strategic Security Report] Navigating the Threat Intelligence Maze

Most enterprises are using threat intel services, but many are still figuring out how to use the data they're collecting. In this Dark Reading survey we give you a look at what they're doing today - and where they hope to go.

[Download Now!](#)
[The State of Ransomware](#)

0 comments

[\[Strategic Security Report\] How Enterprises Are Attacking the IT Security Problem](#)

0 comments

[Twitter Feed](#)
[The Impact of a Security Breach 2017](#)

0 comments

[More Reports](#)

Hayley Scott Retweeted

**Marc Wilczek** @MarcWilczek

7 Deadly Sins to Avoid when Mitigating Cyberthreats: ubm.io/2uqqDps #ITsecurity #cybercrime #databreach @EYnews @DarkReading



Bug Report

Enterprise Vulnerabilities
From DHS/US-CERT's National Vulnerability Database

[CVE-2017-0290](#)

Published: 2017-05-09

NScript in mpengine in Microsoft Malware Protection Engine with Engine Version before 1.1.13704.0, as used in Windows Defender and other products, allows remote attackers to execute arbitrary code or cause a denial of service (type confusion and application crash) via crafted JavaScript code within ...

[CVE-2016-10369](#)

Published: 2017-05-08

unixsocket.c in lxterminal through 0.3.0 insecurely uses /tmp for a socket file, allowing a local user to cause a denial of service (preventing terminal launch), or possibly have other impact (bypassing terminal access control).

[CVE-2016-8202](#)

Published: 2017-05-08

A privilege escalation vulnerability in Brocade Fibre Channel SAN products running Brocade Fabric OS (FOS) releases earlier than v7.4.1d and v8.0.1b could allow an authenticated attacker to elevate the privileges

of user accounts accessing the system via command line interface. With affected version...

[CVE-2016-8209](#)

Published: 2017-05-08

Improper checks for unusual or exceptional conditions in Brocade NetIron 05.8.00 and later releases up to and including 06.1.00, when the Management Module is continuously scanned on port 22, may allow attackers to cause a denial of service (crash and reload) of the management module.

[CVE-2017-0890](#)

Published: 2017-05-08

Nextcloud Server before 11.0.3 is vulnerable to an inadequate escaping leading to a XSS vulnerability in the search module. To be exploitable a user has to write or paste malicious content into the search dialogue.



[About Us](#)
[Contact Us](#)
[Sitemap](#)
[Reprints](#)

[Twitter](#)
[Facebook](#)
[LinkedIn](#)
[Google+](#)
[RSS](#)



Technology Group

Black Hat
Content Marketing Institute
Content Marketing World
Dark Reading

Enterprise Connect
GDC
Gamasutra
HDI

ICMI
[Terms of Service](#) | [Privacy Statement](#) | [Legal Entities](#)
InformationWeek
INsecurity
Interop ITX

Network Computing
No Jitter
Service Management World
VRDC

COMMUNITIES SERVED

Content Marketing
Enterprise IT
Enterprise Communications
Game Development
Information Security
IT Services & Support

WORKING WITH US

Advertising Contacts
Event Calendar
Tech Marketing
Solutions
Contact Us
Licensing